

REMARKS

The Non-final Office Action, mailed May 4, 2007, considered claims 1–33. Claim 1 was objected to because of a typographical error on line 14 of the claim. Claims 2 and 9 were objected to because of the use of the acronym "SSL" without first including a description in plain text. Claims 31–33 were rejected under 35 U.S.C. § 101 as not being directed to non-statutory subject matter. Claims 1, 3–5, 8, 10, 11, 21–30, 32 and 33 were rejected under 35 U.S.C. 102(b) as being anticipated by Traw et al., U.S. Patent No. 6,542,610 (filed Aug. 11, 1997) (hereinafter Traw). Claims 2, 6, 7, 9, 12–20 and 31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Traw.¹

By this response, claims 1–2, 4, 8–9, 11–14, 17, 19, 21, and 31–33 are amended such that claims 1–33 remain pending. Claims 1, 8, 14, 21, 26, and 31–33 are independent claims which remain at issue. Support for the amendments may be found within Specification ¶¶ 49–51.² The Specification has been amended to cure some inadvertent typographical errors.

Claim 1 has been amended to cure the typographical error. Claims 2 and 9 have been amended cure the objection to the use of the acronym "SSL." Claim 31 has been amended to recite physical storage media to cure the rejection of claims 31–33 under 35 U.S.C. § 101 as being directed toward non-statutory subject matter.

As reflected in the claims, the present invention is directed generally toward methods, systems, and computer program products for requesting and providing proof that a system is appropriately configured to access a resource. Claim 1 recites, for instance, in combination with all the elements of the claim, a method which includes receiving a challenge including information indicating how a system is to prove it is appropriately configured to access a resource. The method also includes formulating proof based upon a measurable aspect of the system's configuration that the system's configuration is appropriate for accessing a resource. Finally, the method includes submitting an assertion that can be used to verify that the system is appropriately configured to access the resource.

¹ Although the prior art status of the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

² However, it should be noted that the present invention and claims as recited take support from the entire Specification. As such, no particular part of the Specification should be considered separately from the entirety of the Specification.

Claim 8 is a method similar to that of claim 1 but is recited from the perspective of a providing system as opposed to the perspective of a requesting system as in claim 1.

Claim 14 recites, in combination with all the elements of the claim, a method of generating challenges and pre-computing answers which includes accessing a random value and accessing a secret value. The method includes using the random and secret values to generate a second random value. The method then includes using the first and second random values as input to a hash algorithm to identify one or more regions within a portion of instructions at a computing system. Values are retrieved from the identified regions and an answer to the challenge is pre-computed based on the retrieved values. Claim 31 is a computer program product embodiment of the method of claim 14.

Claim 21 recites, in combination with all the elements of the claim, a method of authorizing a requester to interact with a provider which includes receiving a configuration challenge from the provider which includes information indicating how the requester is to prove that it is appropriately configured to interact with the provider. Proof is formulated based upon a measurable aspect of the requester's configuration that the configuration is appropriate for accessing a resource. Proof of the values of one or more measurable aspects of the requester are sent to the provider. Finally, a token that can be used to prove that the requester is appropriately configured is received. Claim 32 is a computer program product embodiment of the method of claim 14.

Claim 26 recites, in combination with all the elements of the claim, a method which includes receiving a request from a requester. A configuration challenge is caused to be issued to the requester which requests proof that the requester is appropriately configured to interact with the provider. Proof of the values of one or more measurable aspects of the requester's configuration is received and a token is sent that can be used to prove that the requester is appropriately configured.

Concerning independent claim 1:

Claim 1 was rejected under 35 U.S.C. § 102(b) as being anticipated by Traw.³ The Applicants submit, however, that Traw fails to teach each and every element of claim 1 as now recited. In particular, Traw fails to teach accepting a challenge initiated by the providing application, the challenge including information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured to access a resource. Traw teaches only that a *random* challenge is received by either Device A or Device B.⁴ In response to the received random challenge, Traw's devices merely encrypt the random challenge and return the encrypted challenge. Traw fails to teach that the challenge includes information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured. Because the challenge of claim 1 includes information as to how it is to be proven that the computing system is configured, the included information of the present claim is necessarily more than the random challenge as taught by Traw.

Further, Traw fails to teach that the requesting computing system formulates proof, based upon a measurable aspect of a system's configuration, that the measurable aspect of the requesting computing system's configuration is appropriate for accessing a resource. Traw teaches only that a received random challenge is encrypted. However, Traw fails to teach that any proof is formulated based on any measurable aspect of a system's configuration because the random challenge was supplied by another system and the encryption is performed based upon a hash algorithm independent of the system's configuration.

Because, as pointed out above, Traw fails to teach each and every element of the invention as recited in claim 1, a rejection under 35 U.S.C. § 102(b) is improper and should be withdrawn. Accordingly, the Applicants respectfully request favorable reconsideration of claim 1.

Concerning independent claim 8:

Claim 8 was rejected under 35 U.S.C. § 102(b) as being anticipated by Traw.⁵ The Applicants submit that Traw fails to teach each and every element of claim 8 as it is now recited. The method of claim 8 is substantially similar to the method of claim 1 but is recited from the

³ Office Communication pp. 3-4 (paper no. 20070418) (mailed May 4, 2007).

⁴ Traw col. 7 l. 16-41.

⁵ Office Comm. pp. 3, 4-5.

perspective of a providing system as compared to the requesting system of claim 1. Claim 8 has been amended to include limitations similar to those in claim 1 wherein a challenge includes information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured to access a resource and wherein an assertion which can be used to verify that requesting instructions are configured appropriately for interacting with a providing system includes information based at least in part upon the information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured.

As in the discussion of claim 1 above, Traw fails to teach that a challenge includes information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured to access a resource. Traw also fails to teach that a received assertion includes information based at least in part upon both a measurable aspect of how the requesting system is configured and the information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured. Traw teaches only that a random challenge is encrypted and returned but not that an assertion is based upon a measurable aspect of any configuration.

Because Traw fails to teach each and every element of the invention as recited in claim 8, a rejection under 35 U.S.C. § 102(b) is improper and should be withdrawn. Accordingly, the Applicants respectfully request favorable reconsideration of claim 8.

Concerning independent claims 14 and 31:

Claims 14 and 31 were rejected under 35 U.S.C. § 103(a) as being obvious in view of Traw.⁶ The office action notably concedes that Traw fails to disclose four important limitations of the claims: 1) using the first random value and the secret value as input to a first hash algorithm to generate a second random value; 2) an act of using the first random value and the second random value as input to a second hash algorithm to identify one or more regions within a portion of instructions; 3) an act of retrieving values from the identified regions; and 4) an act of pre-computing an answer to the challenge based on the retrieved values.⁷ The Applicants submit that the claim limitations which the office action concedes are not taught by Traw are non-trivial.

⁶ Office Comm. pp. 10–11.

⁷ Office Comm. pp. 10–11.

However, to supply the claim elements which Traw concededly lacks, the office action asserted that:

“ . . . it would have been obvious to one of ordinary skill in the art at the time of invention to use a hash algorithm or any other encryption method when encrypting the first random value with the secret value.”⁸ and “ . . . it would have been obvious to one of ordinary skill in the art at the time of invention to identify regions of the portion instructions as part of the property information about the device being authenticated and retrieve the values from these regions to calculate an answer to the challenge.”⁹

The Applicants submit, however, that the assertions of the office action are insufficient. No reference has been cited nor has any support been provided for the assertions that using a hash algorithm is obvious or that identifying regions of the portion of instructions as part of the property information is obvious. The Applicants disagree that such elements of the claim are obvious. Further, in order to establish a *prima facie* case of obviousness, it is the burden of the Examiner to demonstrate that three criteria are met: first, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and third, *the prior art reference . . . must teach or suggest all the claim limitations*.¹⁰ Because it has not been asserted or shown that Traw teaches or suggests all the claim limitations, *prima facie* case of obviousness has not been asserted and has not been properly supported.

Because the prior art reference (i.e. - Traw) admittedly fails to teach or suggest all the claim limitations, a rejection of claims 14 and 31 under 35 U.S.C. § 103(a) is improper and should be withdrawn. Accordingly, the Applicants respectfully request favorable reconsideration of claims 14 and 31.

⁸ Office Comm. p. 10.

⁹ Office Comm. p. 11.

¹⁰ MPEP § 2143 (emphasis added); *see also In re Royka*, 490 F.2d 981 (CCPA 1974).

Concerning independent claims 21 and 32:

Claims 21 and 32 were rejected under 35 U.S.C. 102(b) as being anticipated by Traw.¹¹ The Applicants submit, however, that Traw fails to teach each and every element of these claims as now recited. The office action asserted that Traw discloses receiving a configuration challenge from the provider, the configuration challenge indicating how the requester is to prove that the requester is appropriately configured to interact with the provider.¹² However, the cited portion of Traw discloses only that "the devices exchange challenges, perhaps random challenges . . . and device certificates" Traw fails to teach that the challenge includes information which indicates how a requestor is to prove that the requestor is appropriately configured to interact. Traw teaches how a devices may be identified, but fails to teach the additional limitation of how a challenge may indicate how a (possibly identified) device is to prove that it is appropriately configured.

Further, Traw fails to teach formulating proof, based upon a measurable aspect of a system's configuration, that the measurable aspect of the requester's configuration is appropriate for accessing a resource. Traw teaches only that a received random challenge is encrypted. Traw fails to teach that any proof is formulated based on any measurable aspect of a system's configuration because the random challenge was supplied by another system and the encryption is performed based upon a hash algorithm independent of the system's configuration.

Because Traw fails to teach each and every element of the invention as recited in claims 21 and 32, a rejection under 35 U.S.C. § 102(b) of those claims is improper and should be withdrawn. Accordingly, the Applicants respectfully request favorable reconsideration of claims 21 and 32.

Concerning independent claims 26 and 33:

Claims 26 and 33 were rejected under 35 U.S.C. 102(b) as being anticipated by Traw.¹³ The Applicants submit, however, that Traw fails to teach each and every element of as recited in the claims. As discussed above, Traw teaches that challenges are exchanged between devices. However, Traw fails to teach that any challenge requests proof that any entity is properly configured. Traw teaches a scheme of identification but, beyond identification, fails to teach any

¹¹ Office Comm. pp. 3, 6.

¹² Office Comm. p. 6.

¹³ Office Comm. pp. 3, 7.

discernment of whether or not any device is appropriately configured. Absent teaching that a challenge includes requesting proof that a requestor is appropriately configured, *inter alia*, Traw fails to teach each and every element of the claims as recited. In view of this, a rejection under 35 U.S.C. 102(b) in view of Traw is improper and should be withdrawn. The Applicants respectfully request favorable reconsideration of claims 26 and 33.

In consideration of the foregoing, the Applicants respectfully submit that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicants acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicants reserve the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicants specifically request that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 3rd day of August, 2007.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorneys for Applicant
Customer No. 47973